

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-171718

(43)Date of publication of application : 26.06.1998

(51)Int.Cl. G06F 12/14
G06K 17/00

(21)Application number : 08-325507

(71)Applicant : NEC CORP

(22)Date of filing : 05.12.1996

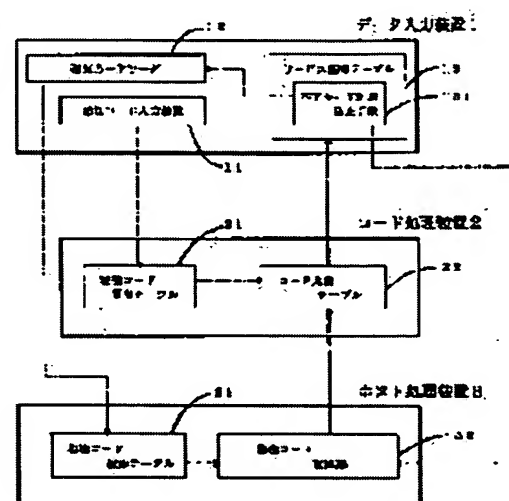
(72)Inventor : WAKAO TAKASHI

(54) METHOD FOR PROTECTING MAGNETIC CARD DATA SECRECY AND DEVICE THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and device for protecting data secrecy for facilitating a countermeasure to illegal use by a person except the owner of a magnetic card.

SOLUTION: A secret code calculated in a constant method by using a password code which can be known only by an owner is preliminarily registered in a secret code storage part 32. When the owner uses a magnetic card, a secret code calculating table 21 calculates a secret code by using an inputted password code. This calculated secret code is compared with the secret code registered in the secret code storage part 32 by a comparing table 22, and judges whether or not the use of the magnetic card is by a legal owner. A service control table 13 controls a magnetic card reader 12 by referring to this judged result.



LEGAL STATUS

[Date of request for examination] 05.12.1996

[Date of sending the examiner's decision of rejection] 28.06.2000

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

Best Available Copy

YqoC sigbolova zrad

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-171718

(43)公開日 平成10年(1998) 6月26日

(51)Int.Cl.⁶

G 0 6 F 12/14

識別記号

3 2 0

F I

G 0 6 F 12/14

3 2 0 C

3 2 0 D

G 0 6 K 17/00

G 0 6 K 17/00

T

審査請求 有 請求項の数4 O L (全 5 頁)

(21)出願番号 特願平8-325507

(22)出願日 平成8年(1996)12月5日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 若生 崇

東京都港区芝五丁目7番1号 日本電気株式会社内

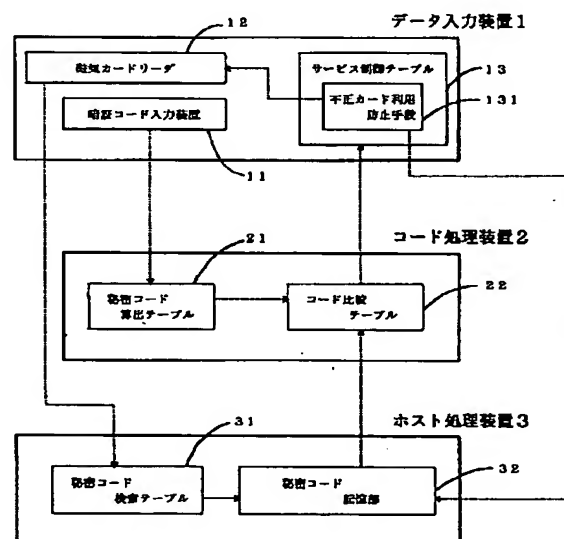
(74)代理人 弁理士 後藤 洋介 (外2名)

(54)【発明の名称】 磁気カードデータ機密保護方法及び装置

(57)【要約】

【課題】 磁気カードの所有者以外の者による不正利用の対策を講じたデータ機密保護方法及び装置を提供すること。

【解決手段】 所有者のみが知り得る暗証コードを用いて一定の方法で算出した秘密コードをあらかじめ秘密コード記憶部32に登録する。所有者が利用する際に入力した暗証コードを用いて秘密コード算出テーブル21が秘密コードを算出する。この算出した秘密コードと秘密コード記憶部32に登録されている秘密コードとをコード比較テーブル22で比較し、磁気カードの利用が正当な所有者であるか否かを判断する。この判断結果を参照して、サービス制御テーブル13が磁気カードリーダー12を制御する。



Best Available Copy

【特許請求の範囲】

【請求項1】 機械的にリード／ライト可能な磁気カードの所有者に与えた暗証コードにより、前記磁気カードの利用に際し正当な所有者であるか否かの確認判断を行い、これにより磁気カードに記録されているデータの機密を保護する磁気カードデータ機密保護方法に於いて、所有者のみが知り得る暗証コードを用いて一定の方法で算出した秘密コードをホスト処理装置にあらかじめ登録しておき、所有者が利用する際に入力した暗証コードを用いてコード処理装置が秘密コードを算出し、前記コード処理装置で算出した秘密コードと前記ホスト処理装置に登録されている秘密コードとを比較し、磁気カードの利用が正当な所有者であるか否かを判断することを特徴とする磁気カードデータ機密保護方法。

【請求項2】 磁気カードには利用者情報が記憶されており、前記両秘密コードが不一致の場合には、使用された磁気カード内の前記利用者情報を消去し、当該磁気カードの再利用を不可能にする請求項1記載の磁気カードデータ機密保護方法。

【請求項3】 機械的にリード／ライト可能な磁気カードの所有者に与えた暗証コードにより、前記磁気カードの利用に際し正当な所有者であるか否かの確認判断を行い、これにより磁気カードに記録されているデータの機密を保護する磁気カードデータ機密保護装置に於いて、所有者のみが知り得る暗証コードを用いて一定の方法で算出した秘密コードをあらかじめ登録する登録手段と、所有者が利用する際に入力した暗証コードを用いて秘密コードを算出する算出手段と、前記算出手段で算出した秘密コードと前記登録手段に登録されている秘密コードとを比較し、磁気カードの利用が正当な所有者であるか否かを判断する比較判断手段とを含むことを特徴とする磁気カードデータ機密保護装置。

【請求項4】 前記両秘密コードが不一致の場合には、使用された磁気カードに記憶されている利用者情報を消去し、当該磁気カードの再利用を不可能にする手段を備えた請求項3記載の磁気カードデータ機密保護装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、磁気カードに記録されているデータの機密を保護する方法及び装置に関する。

【0002】

【従来の技術】従来、磁気カードに記録されているデータの機密を保護するシステムは、例えば、特開昭62-274464号公報または特開昭58-203572号公報に記載されている。それらにおいては、ホスト処理装置の有するデータベース中の磁気カード所有者に関する情報に依存するか、磁気カード内記憶データや所有者の記憶のみに頼った暗証コード等による確認方式を用いる。

【0003】

【発明が解決しようとする課題】しかしながら、現在、ホスト処理装置の有するデータベースへ登録する所有者に関する情報は磁気カード所有者以外の第三者が登録を行う為、該第三者の不正利用が容易に可能であるという重大な問題をもつ。

【0004】また、磁気カード内記憶データと、所有者の記憶する暗証コードとで行う確認方法では、磁気カード内記憶データがカードリーダ等により容易に入手されてしまう為、これも容易に磁気カードの不正利用を可能にしてしまう。

【0005】更に、上述した2種類の問題に於いて、不正利用が可能となった場合は、当該不正利用がエスカレートし、幾度にも渡った不正利用が可能となってしまふ。

【0006】それ故に本発明の課題は、前述した2種類の方法より各々の利点を得、なおかつ所有者以外の者による不正利用の可能性がきわめて少なく、また、不正利用を検知した場合に、該利用に使用された磁気カード内記憶データを消去し、後の更なる悪意的な不正利用を防止する、磁気カードと暗証コードによるデータ機密保護方法及び装置を提供することにある。

【0007】

【課題を解決するための手段】本発明によれば、機械的にリード／ライト可能な磁気カードの所有者に与えた暗証コードにより、前記磁気カードの利用に際し正当な所有者であるか否かの確認判断を行い、これにより磁気カードに記録されているデータの機密を保護する磁気カードデータ機密保護方法に於いて、所有者のみが知り得る暗証コードを用いて一定の方法で算出した秘密コードをホスト処理装置にあらかじめ登録しておき、所有者が利用する際に入力した暗証コードを用いてコード処理装置が秘密コードを算出し、前記コード処理装置で算出した秘密コードと前記ホスト処理装置に登録されている秘密コードとを比較し、磁気カードの利用が正当な所有者であるか否かを判断することを特徴とする磁気カードデータ機密保護方法が得られる。

【0008】また本発明によれば、機械的にリード／ライト可能な磁気カードの所有者に与えた暗証コードにより、前記磁気カードの利用に際し正当な所有者であるか否かの確認判断を行い、これにより磁気カードに記録されているデータの機密を保護する磁気カードデータ機密保護装置に於いて、所有者のみが知り得る暗証コードを用いて一定の方法で算出した秘密コードをあらかじめ登録する登録手段と、所有者が利用する際に入力した暗証コードを用いて秘密コードを算出する算出手段と、前記算出手段で算出した秘密コードと前記登録手段に登録されている秘密コードとを比較し、磁気カードの利用が正当な所有者であるか否かを判断する比較判断手段とを含むことを特徴とする磁気カードデータ機密保護装置が得

られる。

【0009】

【発明の実施の形態】図1は、本発明に実施の形態に係る磁気カードデータ機密保護装置を含むシステムを説明するためのブロック図である。このシステムは、所有者が磁気カードや暗証コードを入力するためのデータ入力装置1と、暗証コードより一定の算出方法にての秘密コードAの算出や当該秘密コードAとホスト処理装置より受信した秘密コードBとの比較を行い利用者の確認を行うコード処理装置2と、磁気カードに記憶されている利用

者情報とそれに対応する秘密コードBを保持し利用者情報より秘密コードBを検索するホスト処理装置3とにより構成されている。

【0010】データ入力装置1は、暗証コード入力装置11と、磁気カードリーダー12と、サービス制御テーブル13とを含んでいる。サービス制御テーブル13は磁気カードリーダー12に接続された不正カード利用防止手段131を有している。

【0011】コード処理装置2は、暗証コード入力装置11に接続された秘密コード算出テーブル21と、この秘密コード算出テーブル21（算出手段）及びサービス制御テーブル13に接続されたコード比較テーブル（比較判断手段）22とを含んでいる。

【0012】ホスト処理装置3は磁気カードリーダー12に接続された秘密コード検索テーブル31と、この秘密コード検索テーブル31、コード比較テーブル22、及び不正カード利用防止手段131に接続された秘密コード記憶部（登録手段）32とを含んでいる。

【0013】先ず、磁気カードの所有者登録時に所有者は4桁の数字で構成される暗証コードを準備し、この暗証コードより秘密コードAを算出するための後述する所定の算出方法（以下、単に「算出法」と呼ぶ）により秘密コードAを算出する。その秘密コードAと所有者情報とを対応させてホスト処理装置へ登録してもらい、磁気カードには所有者情報のみを記憶する。所有者はサービス利用時に該磁気カードを磁気カードリーダー12へ挿入し、次いで所有者のみが知り得る暗証コードを暗証コード入力装置11より入力する。磁気カードリーダー12にて磁気カードから読み取った所有者情報をホスト処理装置3へ転送し、また暗証コード入力装置11より入力された暗証コードをコード処理装置2へ転送する。

【0014】コード処理装置2では、受信した暗証コードより算出法に基づいて秘密コードAを算出する。

【0015】ホスト処理装置3では、磁気カードリーダー12より転送された所有者情報を受信し、秘密コード検索テーブル31にて当該所有者情報を元に秘密コード記憶部32より秘密コードBを検索する。

【0016】更にホスト処理装置3は検索した秘密コードBをコード処理装置2へ転送する。

【0017】次にコード処理装置2はコード比較テ

ブル22にて前述算出した秘密コードAとホスト処理装置3より受信した秘密コードBを比較し、一致不一致により磁気カード利用が所有者であるか否かの確認を行う。

【0018】コード処理装置2は当該結果をデータ入力装置1へ転送し、結果が一致の場合は通常のサービスを開始し、不一致の場合はサービス制御テーブル13により不正カード利用防止手段131を動作させ、磁気カードリーダー12に挿入されている磁気カードの所有者情報を消去する。同時にデータ入力装置1よりホスト処理装置3へ不正利用の通知を行い、ホスト処理装置3は不正利用された磁気カードの所有者情報に対応した秘密コードBにロックをかけ、再度当該所有者情報を受信した場合、対応した秘密コードBを秘密コード記憶部32より引き出せず、通常のサービス利用が不可能になる。

【0019】このようにして、コード処理装置2への算出法の登録者とホスト処理装置3への秘密コードBの登録者が同一人物でない限り、前者は秘密コードを知らず、後者は算出法を知らない為、所有者のみが知り得る暗証コードを用いての不正利用が極めて少ない磁気カード利用のデータ機密保護システムの提供が実現可能となる。

【0020】次に図2を参照して、秘密コード算出テーブル21による算出法を銀行のキャッシュカードを例にとって説明する。まず銀行の口座番号が1526374であり、また所有者の準備した暗証コードが1245である場合には、まずステップ①で暗証コード「1245」を構成する各数字の和「12」を算出する。ステップ②に移り、その和「12」と口座番号「1526374」との積「18316488」を算出する。ステップ③における算出結果を構成する各数字の和「39」をステップ④で算出する。ステップ⑤では、口座番号に連続数字を付随させた所定の表にしたがい、口座番号「1526374」を構成する各数字のどれがステップ③での算出結果「39」に対応するかを見出す。ここでは数字「6」が対応している。ステップ⑥に移り、口座番号「1526374」にその数字「6」を乗じかつ数字「1」を加えて、算出結果「9158245」を得る。この算出結果「9158245」を秘密コードとする。

【0021】

【発明の効果】以上説明したように、本発明によると、暗証コードは磁気カードの所有者のみが知り得るもので、暗証コードより秘密コードを算出する算出法とホスト処理装置に登録されている秘密コードの両方を知り得ない第三者は、暗証コードを知り得ることが不可能なため、所有者の紛失等により当該第三者の手に磁気カードが渡ったとしても、サービスの利用は不可能である。また、該第三者が磁気カードを利用しようとしても、秘密コード不一致により磁気カード内の利用者情報が消去され、照合用のホスト処理装置内秘密コードがロックされるため、該磁気カードを用いたサービスの再利用が不可

能となる。つまり、所有者以外による磁気カードの不正利用を防止し、磁気カードと暗証コードによるデータ機密保護機能を向上させることが可能となる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る磁気カードデータ機密保護装置を含むシステムのブロック図である。

【図2】本発明に於ける秘密コードの算出方法の一例を説明するための説明図である。

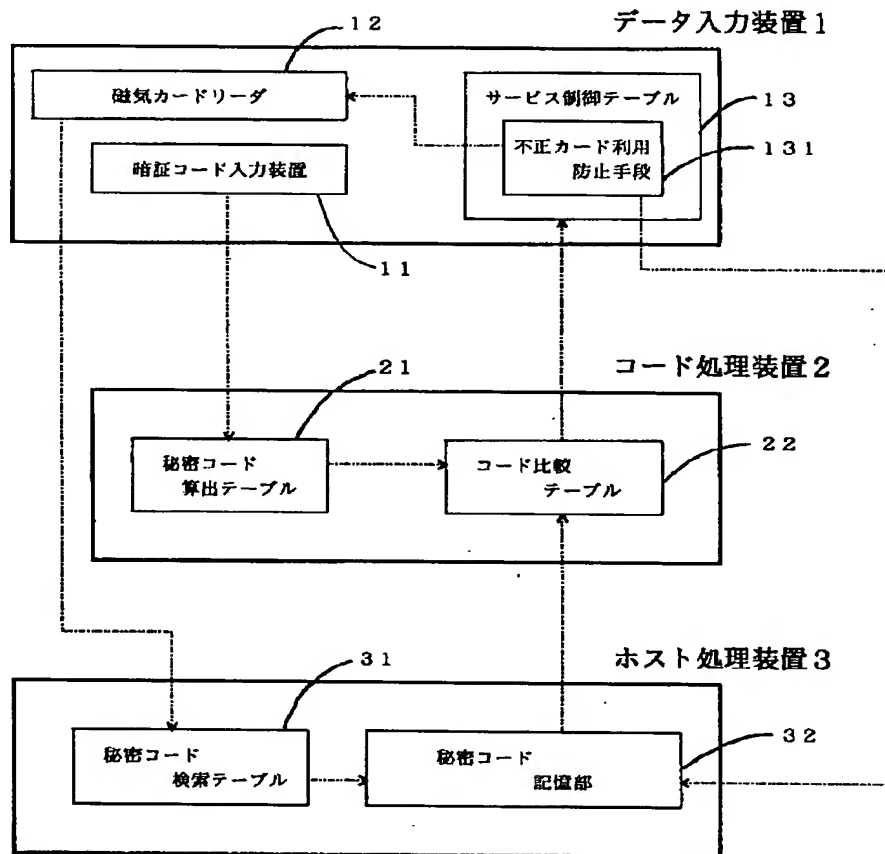
【符号の説明】

1 データ入力装置

*10

- *11 暗証コード入力装置
- 12 磁気カードリーダ
- 13 サービス制御テーブル
- 2 コード処理装置
- 21 秘密コード算出テーブル
- 22 コード比較テーブル
- 3 ホスト処理装置
- 31 秘密コード検索テーブル
- 32 秘密コード記憶部

【図1】



【図2】

<例> 銀行のキャッシュカード

●口座番号 1526374

●暗証コード 1245

①暗証コードより

$$1 + 2 + 4 + 5 = 12$$

②口座番号と

$$1526374 \times 12 = 18316488$$

③その算出結果より

$$1 + 8 + 3 + 1 + 6 + 4 + 8 + 8 = 39$$

④口座番号で

1	5	2		3	7	4
1	2	3	4	5	6	7
8	9	10	11	12	13	14
:	:	:	:	:	:	:
:	:	:	:	:	:	:
36	37	38	39	40	41	42

⑤その数字で工作して

$$1526374 \times 6 + 1 = \underline{\underline{9158245}}$$

THIS PAGE BLANK (USPTO)